MANUAL DE UTILIZAÇÃO

Instrução para uso do Certificado Digital do tipo A3 com MAC OS e Safesign Standart

Sumário

Introdução

O certificado digital está cada vez mais presente em nosso cotidiano, seja em cartão, token ou mesmo diretamente no equipamento – notebook ou desktop.

Nessa instrução, abordamos a instalação e manuseio do certificado em dispositivo cartão mais leitora e token.

Para execução dos testes, utilizamos o Sistema Operacional Mac OS X versão 10.9.4 de 64bits num equipamento de 4 Gb de memória[1] com o navegador Mozilla Firefox versão 31.0 e Gereciador Safesign Standart versão 3.0.88 para MAC OS.

Alguma divergência pode ser observada se a versão do Sistema Operacional e aplicativos forem superior ou inferior ao mencionado nesse documento.

Requisitos necessários

Sistema Operacional Mac OSX ver. 10.9.x;
Navegador Mozilla Firefox ver.30.0 ou superior;
Java 7 ou superior;
Adobe Flash Player;
Gerenciador AET Safesign Standart;
Drive do dispositivo baixado em: http://www.validcertificadora.com.br/faq-mac

[1] Versões de 32bits suportam até 4 Gb (fonte: https://en.wikipedia.org/wiki/Virtual_address_space).

Versão do Sistema Operacional

Versão do Navegador

Versão do Gerenciador

Instalação do Gerenciador Safesign

Acesse a página www.validcertificadora.com.br/faq-mac e realize o download.
Após download do arquivo, descompacte-o, entre na pasta dos arquivos e clique duas vezes sobre **Safesign Macosx** (Figura 1) para abrir o assistente de instalação.

Figura 1

No assistente que iniciar, na tela de **Introdução**, clique em **Continuar**. (Figura 2).

Figura 2

Leia o descritivo de Informação Importante e clique em **Continuar**. (Figura 3).
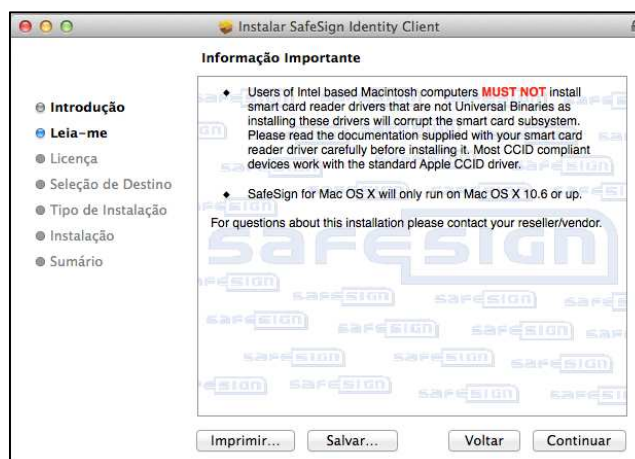
Figura 3

Leia as cláusulas da Licença de uso de Software e clique em **Continuar**. (Figura 4).
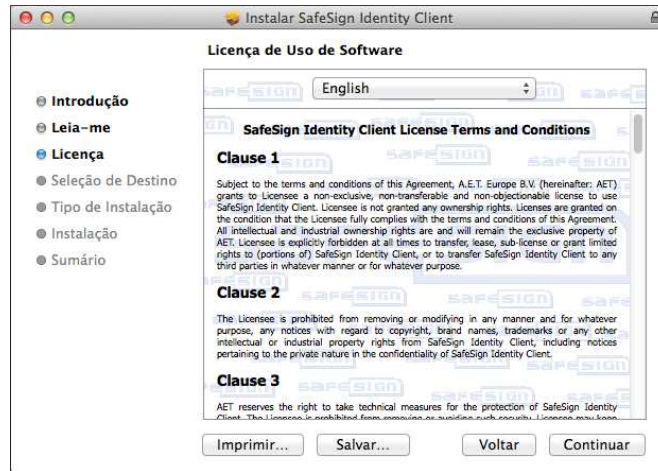
Figura 4

No aviso de concordância com termos de contrato, clique em **Concordar**. (Figura 5).
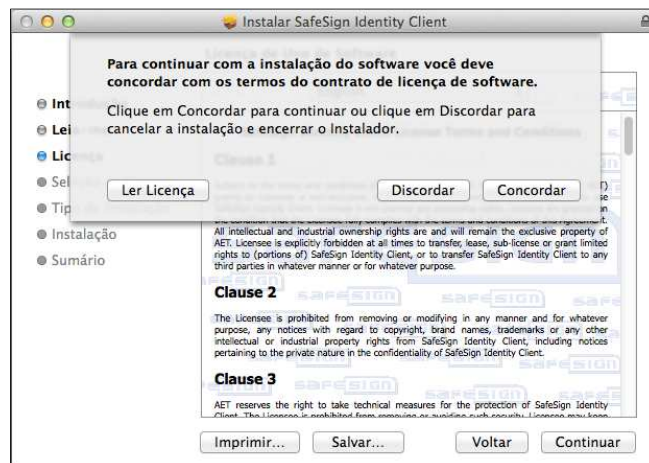
Figura 5

Selecione o local da instalação e clique em **Continuar.** (Figura 6).
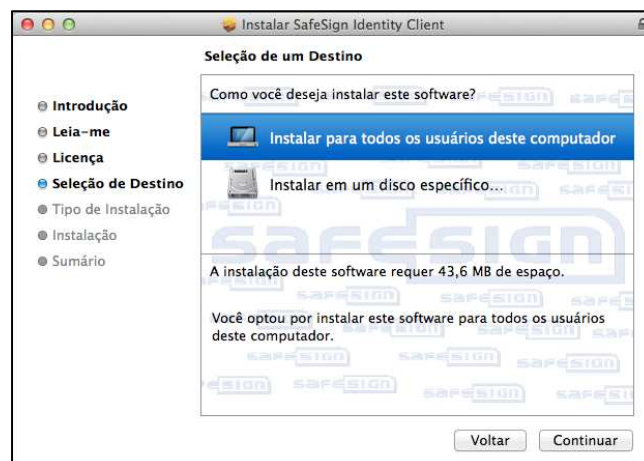
Figura 6

Na tela do Tipo de Instalação, clique em **Instalar** (Figura 7)
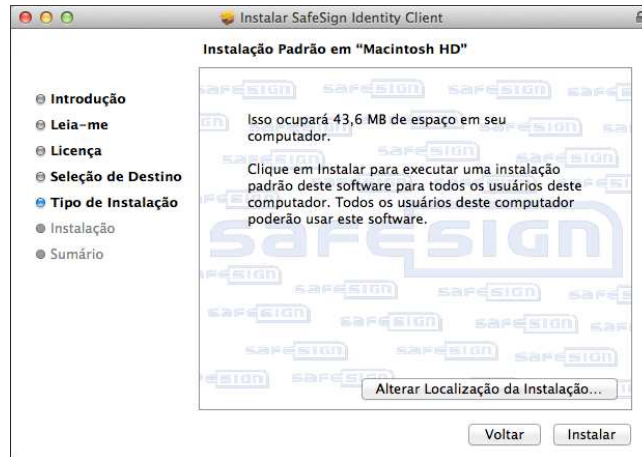
Figura 7

Digite a senha do usuário administrador do sistema e clique em **Instalar Software**. (Figura 8).

Figura 8

Leia o aviso de fechamento da sessão e clique em **Continuar a Instalação**. (Figura 9).
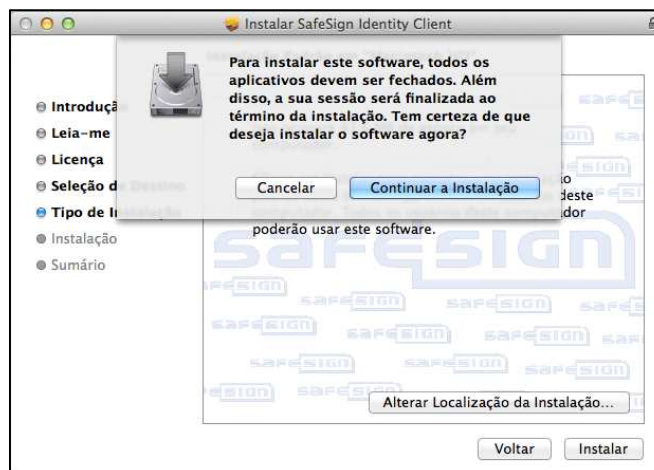
Figura 9

Aguarde o término da instalação. (Figura 10).
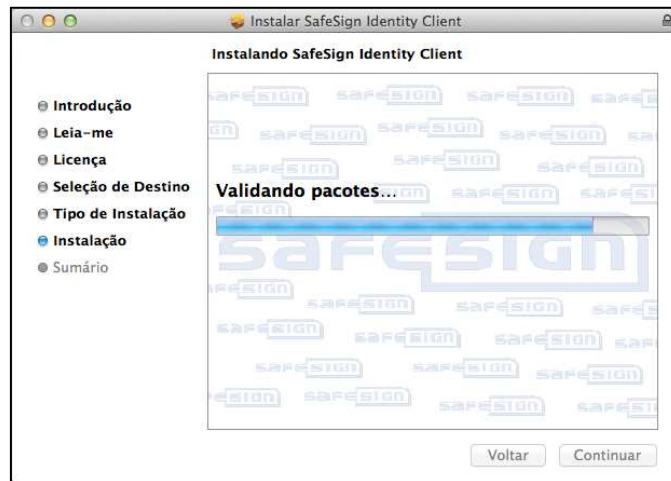
Figura 10

Para concluir a instalação clique em **Finalizar Sessão** na tela de Sumário. (Figura 11). Será finalizada a instalação e aparecerá a tela de logoff.
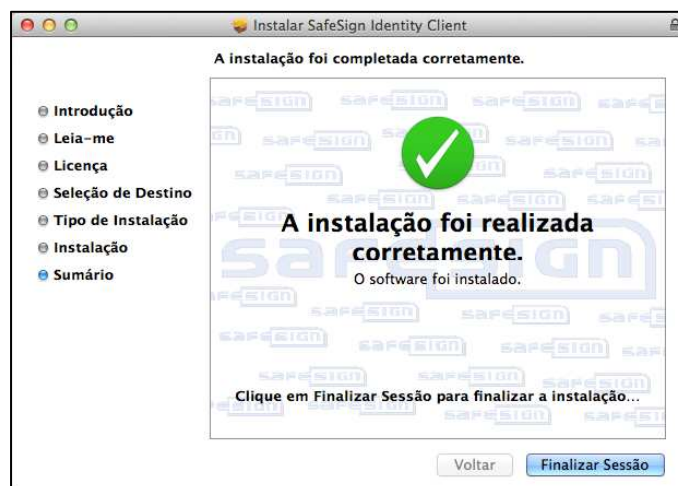
Figura 11

Pronto! Conecte a leitora na porta USB e insira o cartão nela. Vá até a sessão de aplicativos e encontre o ícone **tokenadmin** (Administração do token). Abra-o e aguarde o status ficar **operacional**. (Figuras 12 e 13).

Figura 12
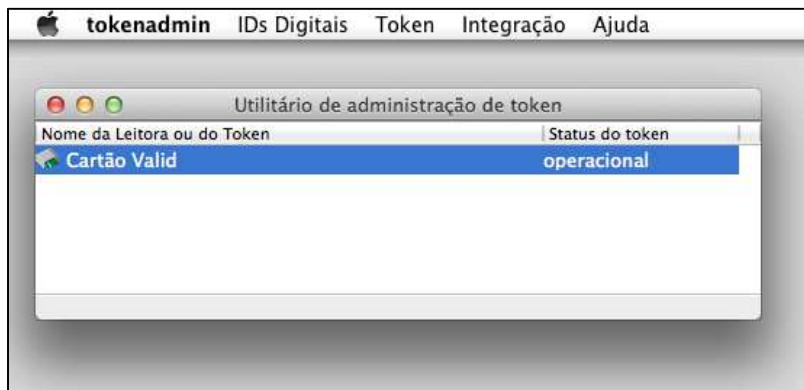
Figura 13

Clique duas vezes sobre o Nome da Leitora ou token (na figura 13 como Cartão Valid) com status operacional para ver seu conteúdo. (Figura 14).
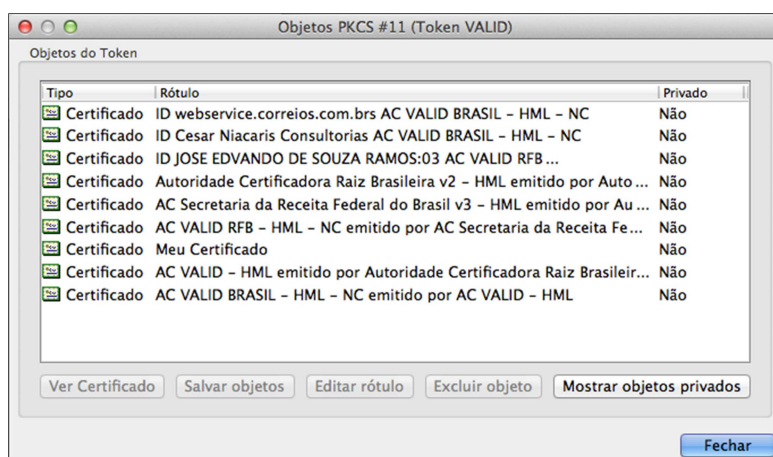
Figura 14

Instalação do token G&D

Para usar o certificado emitido em token, instale primeiro o **Gerenciador Safesign** (tokenadmin - Utilitário de administração do token) descrito acima e em seguida o driver do token mostrado a seguir. Clique duas vezes sobre o ícone **Starsign driver MacOSX** para iniciar a instalação. (Figura 15).

Figura 15

Digite a senha do usuário administrador do sistema e clique em **OK**. (Figura 16).
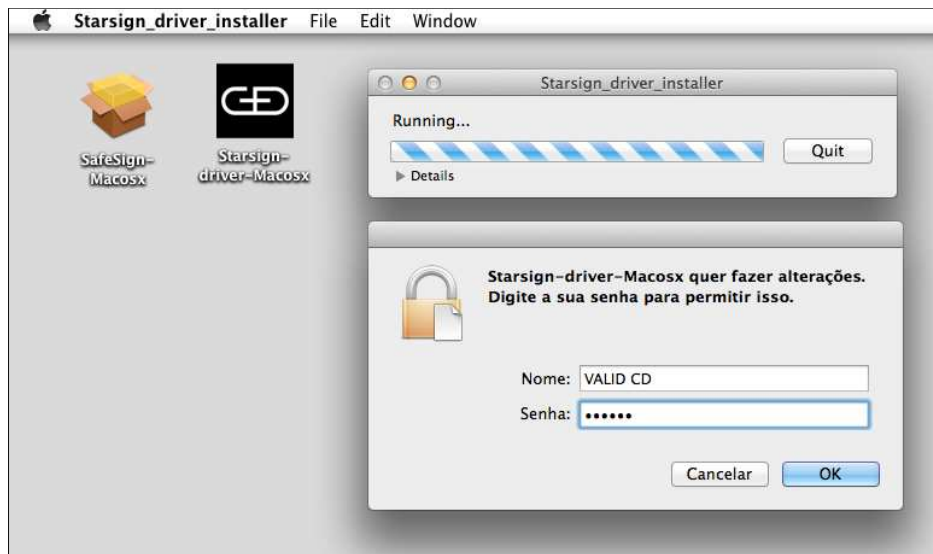
Figura 16

Para finalizar a instalação clique em **Quit** (Sair). (Figura 17).
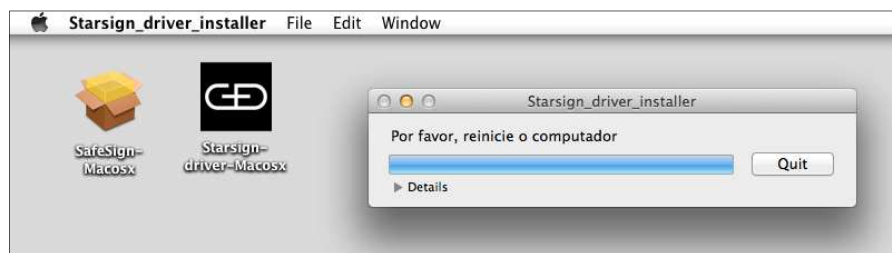
Figura 17

Pronto! Conecte o token na entrada USB. Vá até a sessão de aplicativos e encontre o ícone **tokenadmin** (Administração do token) (Figura 12). Abra-o e aguarde o status ficar **operacional**. (Figura 18).
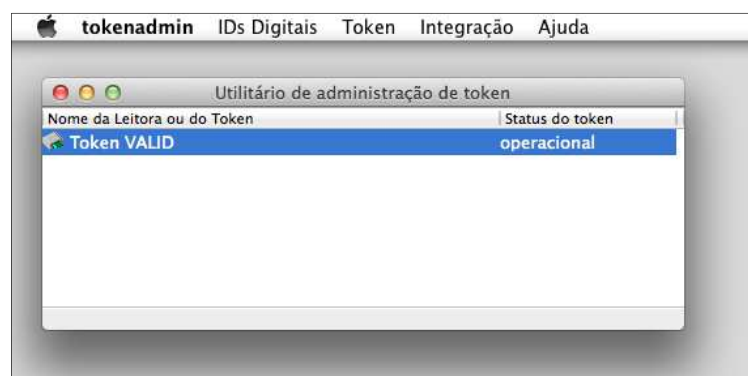
Figura 18

Importante: se o navegador **Firefox** já está instalado no equipamento, o assistente mostrará a opção para instalar o Safesign no Firefox. O mesmo procedimento pode ser feito também pelo **Menu Integração**. Veja a seguir:

Instalação do Safesign no navegador Firefox

Com o **tokenadmin** (Administração do token) aberto, clique no menu **Integração** e depois em **Instalar o Safesign no Firefox...** (Figura 19).
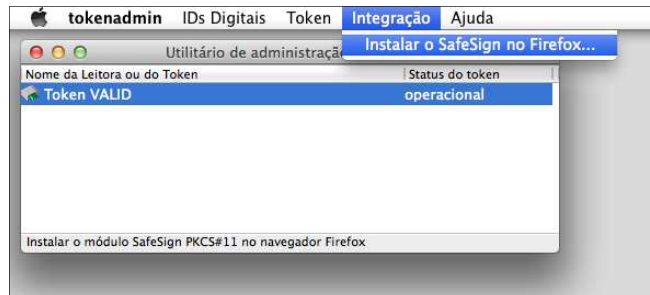
Figura 19

Clique em Instalar e em seguida **OK** na mensagem de **Sucesso** que abrir. (Figura 20).

Importante: se na tela de seleção do navegador não identificar nenhum Firefox, vá para o tópico **Configurar Safesign no navegador Firefox** e siga os passos de configuração.
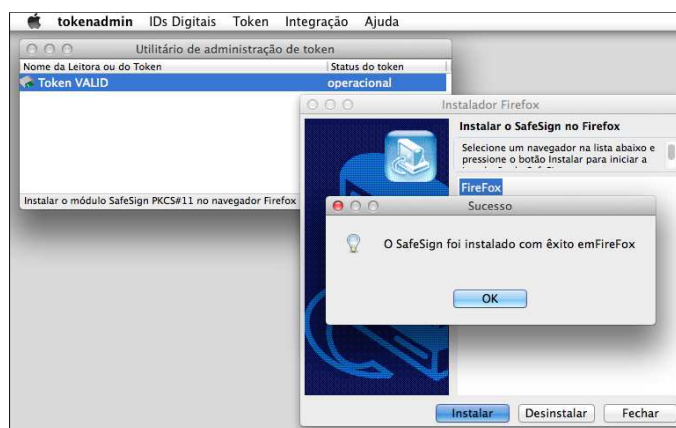
Figura 20

Pronto! Agora Já pode configurar a biblioteca no navegador. Feche a janela do assistente e acompanhe o próximo passo. (Figura 21).
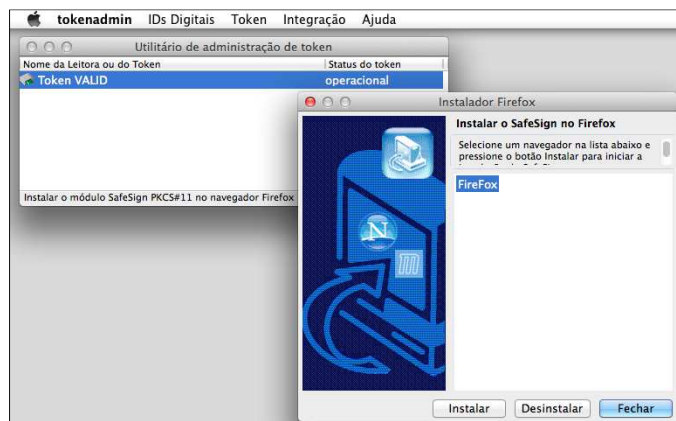
Figura 21

Configurar Safesign no navegador Firefox

Com o navegador aberto, clique no menu **Firefox** e depois na opção **Preferences...** (Figura 22).

Figura 22

Na janela que abrir clique no ícone **Advanced** (Avançado), em seguida na aba **Certificates** (Certificados) e depois no botão **Security Devices** (Dispositivos de segurança). (Figura 23).
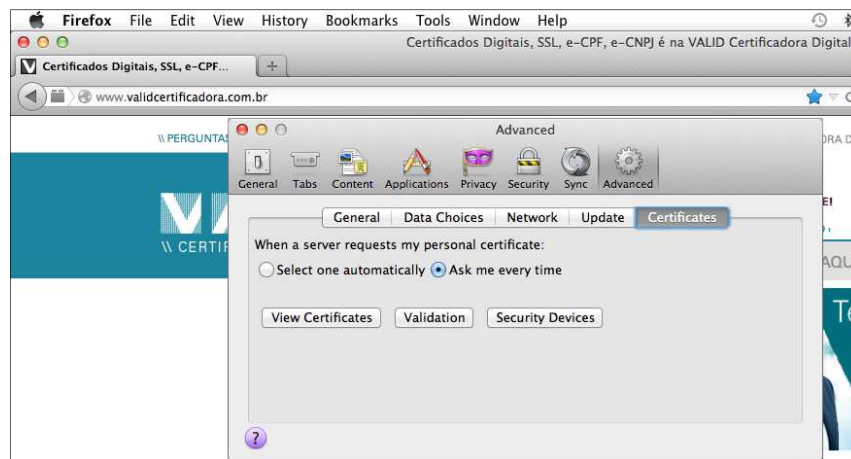
Figura 23

Na janela de **Device Manager** (Gerenciador de Dispositivos), clique no botão **Load** (Carregar). (Figura 24).
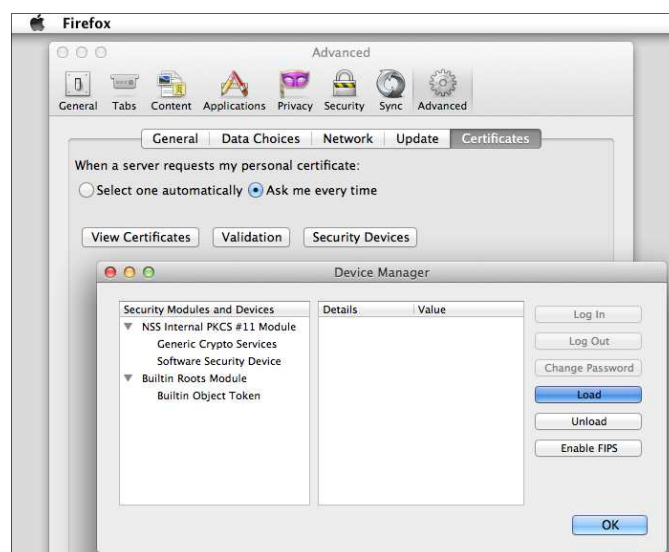
Figura 24

Nos campos de informações do módulo, digite **Safesign** no campo Module Name (Nome do módulo) e seu nome de arquivo **libaetpkss.dylib**. Clique em **OK**. (Figura 25).
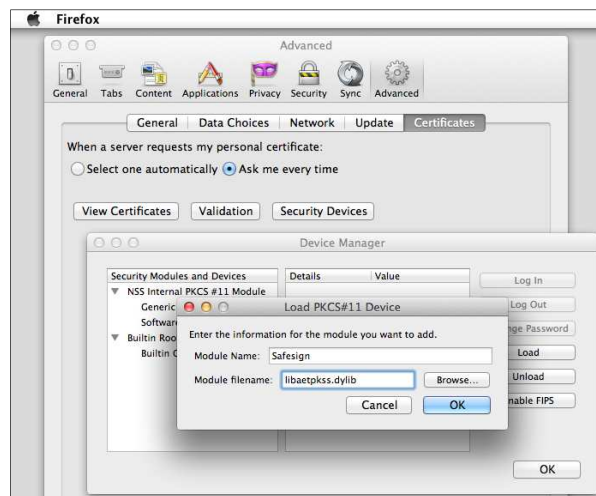
Figura 25

Pronto! O módulo está identificado e carregado. Clique em **OK** para concluir. (Figura 26).
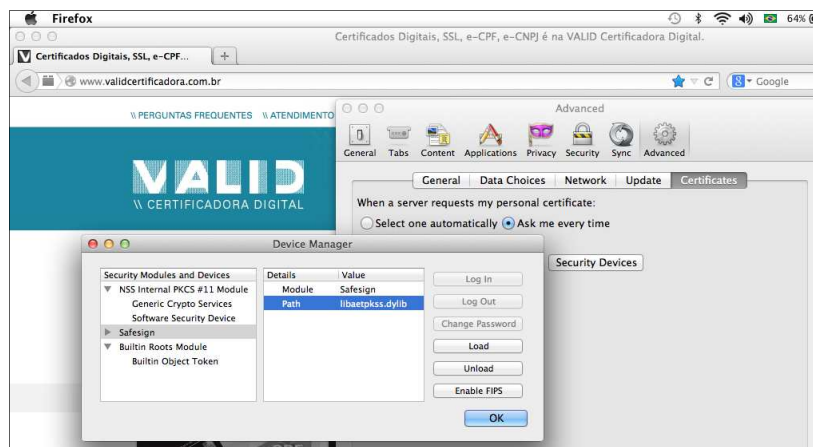
Figura 26

Com o dispositivo conectado (cartão e leitora ou token), o navegador identifica-o e solicita a digitação do PIN. (Figura 27).
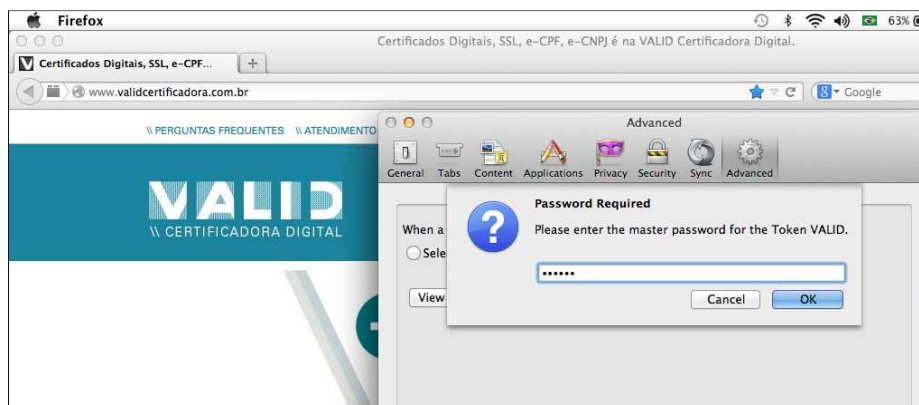
Figura 27

Pronto! O certificado foi publicado no navegador e está pronto para utilização. (Figura 28).
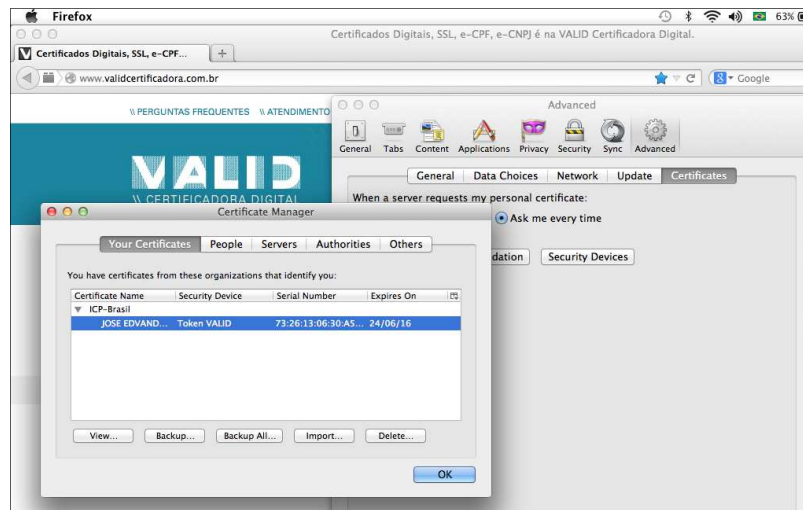
Figura 28

Exemplo de acesso ao Portal e-CAC da Receita Federal

Com o navegador aberto, entre no site da Receita Federal e na sessão **Acesso ao eCAC**, clique no botão **Certificado Digital**. (Figura 29).

Figura 29

Digite o PIN do dispositivo e clique em **OK**. (Figura 30).

Figura 30

Selecione o certificado que acessará o Portal e-CAC na lista de certificados. Pode ser que o dispositivo (cartão ou token) contenha mais de um certificado. Clique em **OK**. (Figura 31).
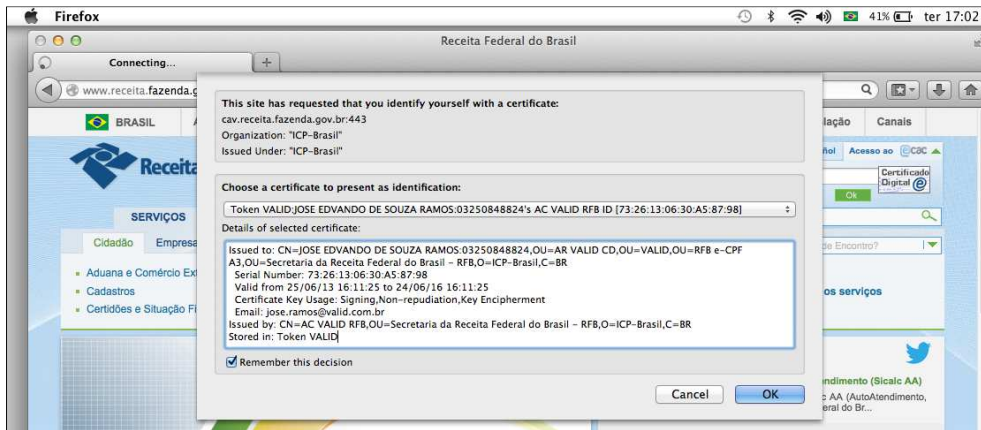
Figura 31

Pronto! Acesso ao portal efetuado com sucesso. (Figura 32).

Figura 32

Nota Importante: Se for o primeiro acesso ao Portal do e-CAC com certificado digital, aparecerá o aviso de segurança do site. Siga o assistente e adicione a exceção, publicando o certificado do portal no navegador. Veja as imagens a seguir:

Após clicar no botão **Certificado Digital** da sessão **Acesso ao e-CAC**, o navegador mostrará o aviso de segurança. (Figura 33).
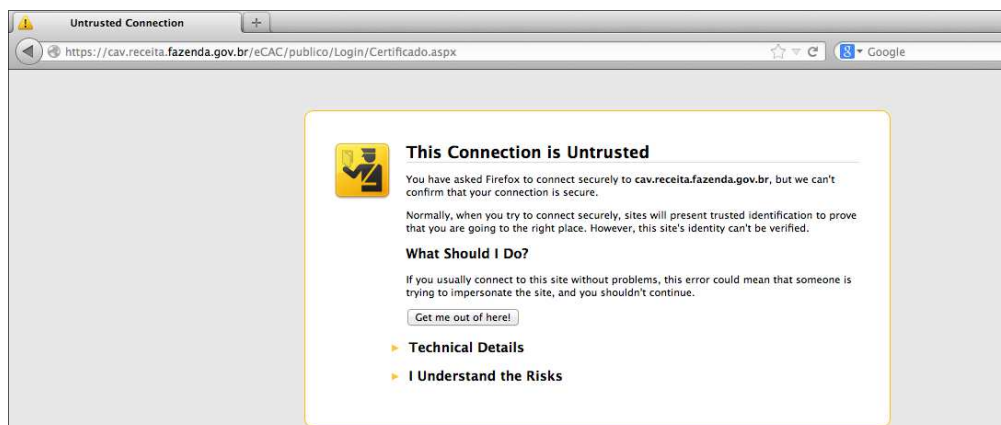
Figura 33

Clique na opção **I Understand the Risks** (Eu Entendo os Riscos) e depois no botão **Add Exception...** (Adicionar Exceção). (Figura 34).
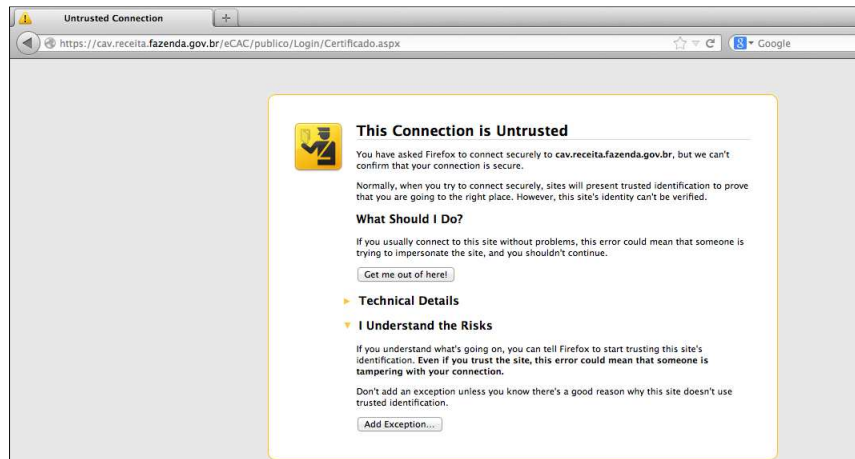
Figura 34

Confirme a inclusão clicando no botão **Confirm Security Exception** (Confirmar exceção de Segurança). (Figura 35).
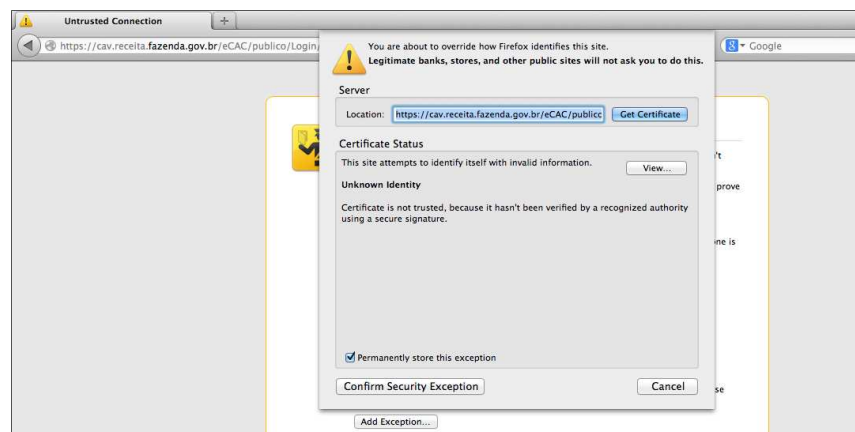
Figura 35

Digite o PIN do dispositivo e clique em OK. (Figura 36)
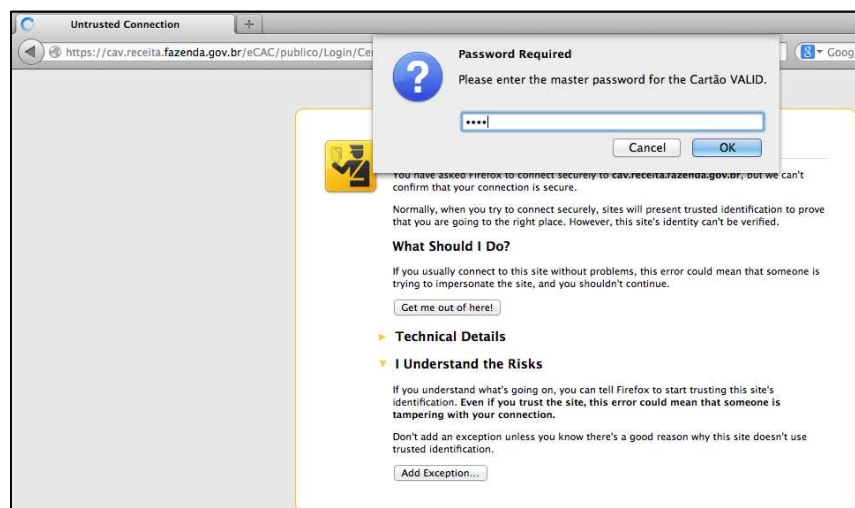
Figura 36

Selecione o Certificado que acessará o Portal e-CAC na lista de certificados. Pode ser que o dispositivo (cartão ou token) contenha mais de um certificado. Clique em **OK**. (Figura 37).
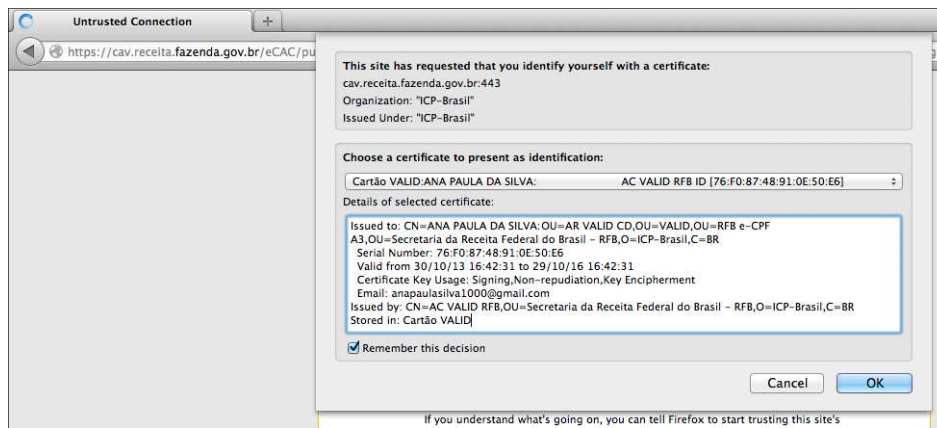
Figura 37

Pronto! Acesso ao portal efetuado com sucesso. (Figura 38).

Figura 38

VALID Certificadora Digital
Classificação: **PÚBLICO**
Para maiores informações acesse
www.validcertificadora.com.br

Agosto de 2014